Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2025-30065: A Ticking Time Bomb in Apache Parquet

Date of Publication	Admiralty Code	TA Number
April 8, 2025	A1	TA2025104

Summary

First Seen: April 2025
Affected Products: Apache Parquet
Impact: A critical remote code execution (RCE) vulnerability, tracked as CVE-2025-30065 with a maximum CVSS score of 10.0, has been uncovered in all versions of the Apache Parquet Java library. This flaw could allow attackers to gain full control over a system simply by tricking it into processing a maliciously crafted Parquet file. Once exploited, the vulnerability could let attackers execute arbitrary code, steal or manipulate sensitive data, and install malware undetected. Given the severity of the issue, users are strongly urged to upgrade to Apache Parquet version 1.15.1, which addresses and resolves the flaw.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-30065	Apache Parque Remote Code Execution Vulnerability	Apache Parquet	✗	✗	✓

Vulnerability Details

#1 A critical vulnerability, tracked as CVE-2025-30065 and carrying the highest CVSS score of 10.0, has been discovered in Apache Parquet's Java library. The flaw stems from deserialization of untrusted data, a weakness that could allow remote code execution (RCE) if a specially crafted Parquet file is processed by a vulnerable system. Once exploited, attackers could take control of affected systems, steal or tamper with sensitive data, or silently install malware making this a severe threat with far-reaching consequences.

#2 Apache Parquet is a popular open-source columnar storage format that serves as the backbone for many big data and analytics platforms. It's deeply integrated into processing frameworks like Apache Hadoop and Spark, and is widely used across major cloud providers including AWS, Google Cloud, and Azure. Because of its widespread use, this vulnerability poses a significant risk to a vast number of enterprise data pipelines and analytics environments.

#3 The vulnerability affects all versions up to 1.15.0. Adding urgency to the situation is the fact that a proof-of-concept (PoC) exploit has already been made public, increasing the likelihood of active attacks. To mitigate the risk, users must upgrade to Apache Parquet version 1.15.1, which fully patches CVE-2025-30065. With exploitation now possible and widespread adoption of Parquet in modern data environments, this is a priority patch for anyone in the data engineering or analytics space.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-30065	Apache Parquet Version 1.15.0 and Prior	cpe:2.3:a:apache:parquet:*:*:*:*:*:*	CWE-502

Recommendations

Upgrade Immediately : Make sure you update your systems to Apache Parquet Java library version 1.15.1 right away. This update fixes a serious security flaw that could let hackers run harmful code on your systems if left unpatched.

Audit Your Software Stack: Take a close look at your apps, data pipelines, and ETL tools to see if they use the Apache Parquet Java library especially versions between 1.8.0 and 1.15.0. Don't overlook cloud services, third-party analytics tools, or any custom-built software that might rely on it.

Be Cautious with External Parquet Files & Watch for Suspicious Activity: Treat all Parquet files from outside sources as untrusted validate and sandbox them before processing to avoid triggering the vulnerability. At the same time, monitor your data systems for unusual behavior like strange file downloads, odd API calls, or unknown binaries running. Set up alerts in your SIEM to catch any signs of exploitation early.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0002** Execution	**TA0040** Impact	**T1588** Obtain Capabilities
T1588.006 Vulnerabilities	**T1059** Command and Scripting Interpreter	**T1529** System Shutdown/Reboot	**T1203** Exploitation for Client Execution

Patch Details

To safeguard against the CVE-2025-2783 vulnerability, Patch your systems by upgrading to Apache Parquet Java library v1.15.1.

Link: https://dist.apache.org/repos/dist/release/parquet/apache-parquet-1.15.1/

References

https://www.openwall.com/lists/oss-security/2025/04/01/1

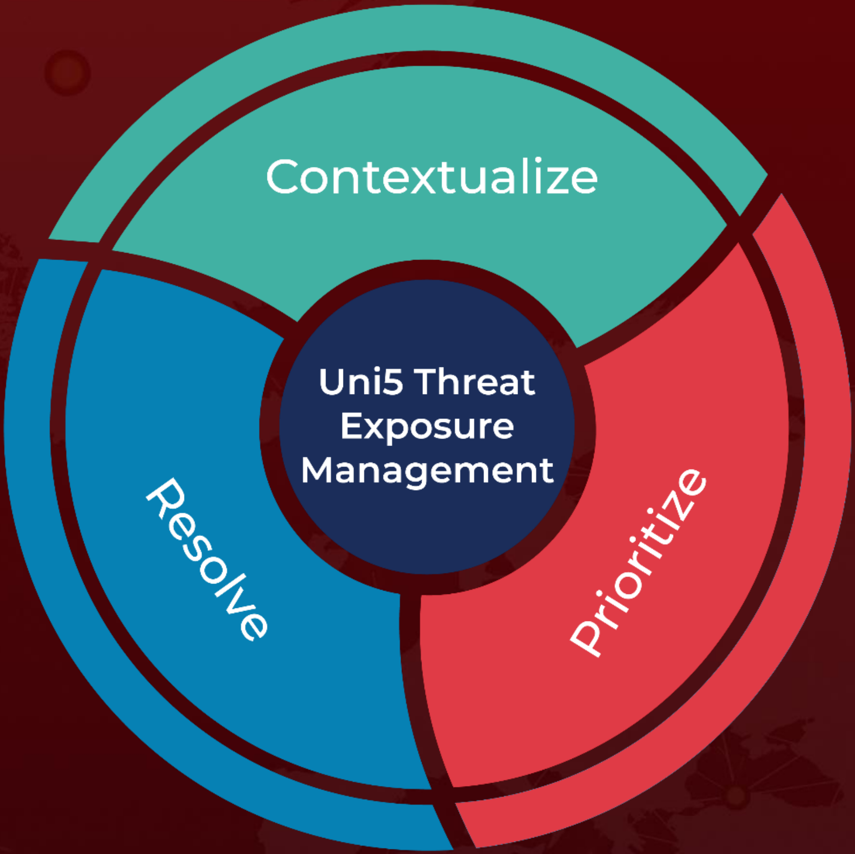
https://github.com/h3st4k3r/CVE-2025-30065

https://techcommunity.microsoft.com/blog/microsoftdefendercloudblog/guidance-for-handling-cve-2025-30065-using-microsoft-security-capabilities/4401362

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 8, 2025 • 5:00 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com